The National Cybersecurity Initiative (NCI):
Securing Nigeria's "Cyberspace" for Economic Development & Growth

Basil Udotai, Esq.
Coordinator,
Nigerian Cybercrime Working Group (NCWG)

CTO 2005

Muson Center, Onikan

May 16 – 20, 2005

The National Cybersecurity Initiative (NCI) What is this about?

- The creation of a sanction-based approach to:
- Securing of Computer Systems and Networks; and
- Protecting Critical ICT infrastructure in Nigeria

The Nigerian Cybercrime Project Background

- Presidential Committee on Cybercrime
- Report recommended creation of a legal and institutional framework for cybercrime in Nigeria
- Create a central agency to enforce cybercrime or situate responsibility within existing law enforcement institution
- Create the Nigerian Cybercrime Working Group (NCWG) as an inter-agency body of law enforcement, intelligence, security and ICT institutions, plus private sector
- Proposed a Draft Nigerian Computer Security and Protection Act

The Nigerian Cybercrime Working Group (NCWG)

- an Inter-Agency body made up of all key law enforcement, security, intelligence and ICT Agencies of government, plus major private organizations in the ICT sector; including Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC); Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS); Nigeria Internet Group (NIG); Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen representing public interest. 2 Chairman and one Coordinator.

- ToR include public enlightenment – CYBERSECURITY FORUM for the Financial Services Sector, building institutional consensus amongst existing Agencies, providing technical assistance to the National Assembly on Cybercrime and the Draft act; laying the groundwork for establishment of institutional capacity in Nigeria, etc.

- Commencement of Global cybercrime enforcement relations – CCIPS (USA), NHTCC (UK), NPA (SA)

Draft Nigerian Computer Security and Protection Act

- **Substantive – criminalize conducts against ICT systems, using ICT systems and targeting critical ICT infrastructures**
- **Procedure – judicial procedures for investigation and prosecution**
- **Including data retention obligations on all ISPs, TSPs, ASPs [periods of data retention and nature of data to be agreed between Govt and industry]**
- **Constructively amend all traditional Intellectual Property laws and the Evidence Act: not just legal enforceability, but also prohibiting the production and distribution of devices manufactured specifically to circumvent security measures for protecting software against copying**
- **Establish institutional framework for enforcement in Nigeria**
- **Creating global law enforcement cooperation with international law enforcement organizations Worldwide**

Projects

- A key mandate for NCWG is forging a Legal and Institutional framework for securing computer systems and networks in Nigeria and protect critical ICT infrastructure in the country
- However, we are undertaking a few preliminary projects that border on Cybercrime and Cybersecurity:
- Official Document Authentication
- Internet Exchange Program
- Cybersecurity Assistance Center (CAC)
- Registration with the G8 24/7 Network
- Reclaim of Official-Looking and Misleading Domain Names with ICANN
- Computer and Network Security Standardization
- National Cybersecurity Policy
- Mutual Legal Assistance Treaty (MLAT);
- Computer Emergency Response Team (CERT) Program;
- Lawful Interception Technology (LIT);
- International Best Practice
- ECOWAS Cybersecurity Protocol

Operational Architecture

- A single central infrastructure for media interception, data analysis and dissemination to all Law Enforcement, Security and Intelligence Agencies in Nigeria;
- The intercept hub into which all law enforcement agencies in Nigeria will interconnect

CYBER SECURITY

- Confidentiality, Integrity and Survivability (CIS)

- There are at least 2 aspects:
- 1. Technology of Cyber Security; and
- 2. Law of Cyber Security

Technology of Cyber Security

- All the solutions – hardware, software and everything in between, aimed at securing computer systems and networks
- Is technological solutions truly able to secure computer systems and networks?
- “There is no such thing as a SECURE network” – Yale Cybercrime Conference 2003

Law of Cyber Security

- **Legislation** – laws against illegal online activities - unauthorized access or access exceeding authorization; network intrusion; denial of service; intellectual property theft; password sharing; dealing in decoding devices, etc;
- **Rules and Regulation** – specify judicial and evidential procedures for bringing electronic cases to court; also some regulations could require network security insurance for certain types of networks – usually critical information infrastructure
- **Transactions** – contractually attributing clear responsibilities and liabilities to all players in today's mostly **multiple player platform**

How crucial is the law of cyber security?

- A critical requirement for eReadiness!
- "E-readiness" is a measure of the extent to which a country's business environment is conducive to technology based commercial opportunities – United Nations
- Many factors are considered in eReadiness ranking of countries, but the most important are: National ICT Standards, Regulations and enforceable Cyber laws …
- One of the most important factors hindering developing countries from achieving maximum economic potential from ICT, includes the absence of adequate legal and regulatory frameworks - UNCTAD/SDTE/ECB/2003/1

Is this possibly true?

- Digital Divide
- Cyber Security
- Digital Opportunities

What Law?

- What law?

  It is NOT a crime in Nigeria except conduct is prohibited in a written law in which a punishment is also prescribed

- Conduct Prohibition Requirements - CFRN;

  Even where conduct amounts to a crime in Nigeria, the acts criminalized may not be punished except a judicial process exists where evidential rules enable trial and conviction of offender

– Legal Consequences Requirements.

Why Substantive Law is Necessary

- Technology does not provide absolute security or protection;
- Law to bridge the gap: Technology + Liability = PROSECUTION
- International Law Enforcement Assistance = “Dual Criminality Requirements” – “I LOVE YOU” virus led to the enactment of Cybercrime laws in the Philippines,
- Official institutional authority to enforce law, handle CERT (UK Air Control System 2hr downtime, UKHTCC to the rescue!) and execute bilateral (MLATs) and multilateral treaties (CoE Cybercrime Convention)

Why now?

- eReadiness Ranking - Do we need more excuse?
- Constitutional prerogative of government to enforce law: sophistication of crime or high-tech nature of media not excuse for inaction;
- Success in ICT in Nigeria = Fastest growing telecoms market in Africa – ITU, more than $10 billion FDI in 4 yrs and 10 million subscribers (NCC);
- Increasing dependence on ICT: personal, business and government;
- Telecoms infrastructure critical to Nigeria's economic and social well being;
- Damage will have more expansive effects, with grave social, economic and political consequences;
- Telecoms is a "test case" for other FDI

Global Trends
What are other countries doing?

- Enacting legislation – substantive and procedural laws that criminalize certain activities online and create procedures for investigation, prosecution, punishment and sentencing of offenders, while enhancing global collaboration in cybercrime and cybersecurity enforcements

- US, UK, and SA – laws affecting Computer Misuse, Computer Privacy, Electronic Transactions, Computer Crimes, Computer Security Enhancement, Data Retention Laws, Digital Signatures and Computer Evidence Laws

- Internationally: G8 24/7 Network; CoE Convention on Cybercrime – now Treaty open to non – European signatories – USA, Japan, South Africa, etc have signed – model, generally acceptable worldwide; OECD, WTO, UNCTAD, UNCITRAL, etc

Who are we kidding!

The issue with eCommerce in Nigeria is not about enforceable law but about 419!

419 is a tussle between **perception** and **reality**

Taking steps to influence the **reality** positively will over time impact the **perception**

Conclusion

Enforcing cybercrime and insisting on cybersecurity in Nigeria are necessary compliments to the great strides by Government to transform Nigeria into an ICT – driven economy. To do otherwise is to deliberately endanger the same infrastructures we have worked so hard and invested so much to build;

Absence of Cybercrime Enforcement constitutes a real HURDLE to launch of full-fledged eCommerce in Nigera; and may be the real reason why ICT outsourcing is hindered.

THANK YOU

CONTACT:

Nigerian Cybercrime Working Group (NCWG)

Office of the National Security Adviser

Three Arms Zone

Aso Rock Villa

Abuja

09 222 3000;

GSM 0803 306 6004

b.udotai@cybercrime.gov.ng

www.cybercrime.gov.ng